PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-003256
(43)Date of publication of application : 06.01.1998

(51)Int.Cl. G09C 1/00
G09C 1/00
G09C 1/00
G11B 20/10
H04L 9/08
H04L 9/06
H04L 9/14

(21)Application number : 08-269502
(22)Date of filing : 11.10.1996

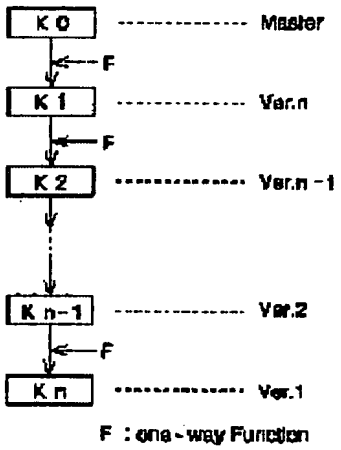
(71)Applicant : SONY CORP
(72)Inventor : ISHIGURO RYUJI

(30)Priority

Priority number	Priority date	Priority country
07267249	16.10.1995	JP
07267250	16.10.1995	
08 93800	16.04.1996	JP
		JP

(54) CIPHERING METHOD AND DEVICE THEREFOR, RECORDING METHOD, DECODING METHOD AND DEVICE THEREFOR AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To easily control the ciphering key.
SOLUTION: A ciphering key K1 is generated from a master key K0 using a unidirectional function, a next ciphering key K2 is generated from the key K1 using the function and similarly n-hierarchial ciphering keys K1 to Kn are generated. Then, information is ciphered by the key Kn and the information is decoded by the ciphering key Kn. If the key Kn is read, the information is ciphered by the key Kn-1 and the information is decoded by the key Kn-1. Thus, the information, which is ciphered by the key Kn, is decoded by the key Kn obtained from the key Kn-1 using the function and the user is only required to maintain the latest key Kn-1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－3256

(43)公開日　平成10年(1998)１月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ａ
		６１０	7259－5Ｊ			６１０Ｂ
		６６０	7259－5Ｊ			６６０Ｄ
			7259－5Ｊ			６６０Ｅ
Ｇ１１Ｂ	20/10		7736－5Ｄ	Ｇ１１Ｂ	20/10	Ｈ

審査請求　未請求　請求項の数28　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平8－269502

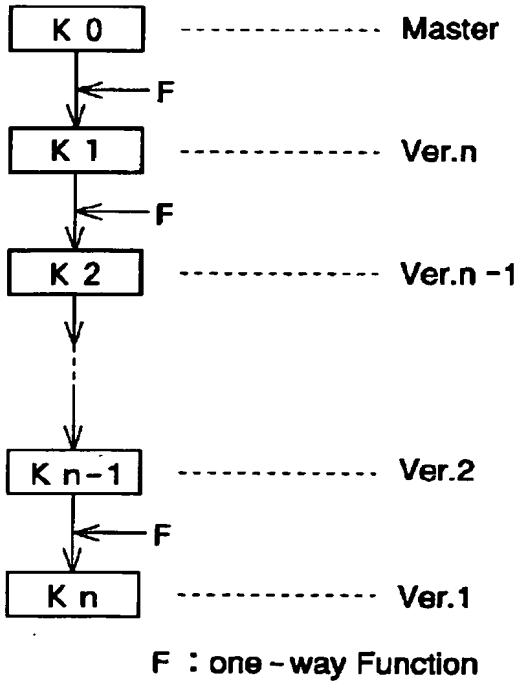
(22)出願日　平成８年(1996)10月11日

(31)優先権主張番号　特願平7－267249
(32)優先日　平７(1995)10月16日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平7－267250
(32)優先日　平７(1995)10月16日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平8－93800
(32)優先日　平８(1996)４月16日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体

(57)【要約】
【課題】　暗号化キーの管理を容易にする。
【解決手段】　マスタキーＫ０から一方向関数を用いて暗号化キーＫ１を作成し、暗号化キーＫ１から一方向関数を用いて次の暗号化キーＫ２を作成し、同様にしてｎ階層の暗号化キーＫ１乃至Ｋｎを作成する。暗号化キーＫｎにより情報を暗号化し、この情報を暗号化キーＫｎで復号化する。暗号化キーＫｎが解読された場合、暗号化キーＫｎ－１を用いて情報を暗号化し、この情報を暗号化キーＫｎ－１で復号化する。暗号化キーＫｎで暗号化された情報は、暗号化キーＫｎ－１から一方向関数を用いて求めた暗号化キーＫｎで復号化することができ、ユーザは最新の暗号化キーＫｎ－１だけを保持すればよい。



1

【特許請求の範囲】

【請求項１】　所定の情報を所定の暗号化キーを用いて暗号化する暗号化方法において、
上記暗号化キーを一方向関数を用いて階層化し、
上記階層化された暗号化キーを用いて上記所定の情報を暗号化することを特徴とする暗号化方法。

【請求項２】　階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであることを特徴とする請求項１に記載の暗号化方法。

【請求項３】　上記階層化された暗号化キーを用いて特定情報を暗号化することを特徴とする請求項１に記載の暗号化方法。

【請求項４】　暗号化された所定の情報を記録媒体に記録する記録方法において、
一方向関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を受信し、
上記暗号化された所定の情報を上記記録媒体に記録することを特徴とする記録方法。

【請求項５】　上記暗号化キーを用いて暗号化された特定情報を受信し、
上記暗号化された所定の情報とともに上記暗号化された特定情報を上記記録媒体に記録することを特徴とする請求項４に記載の記録方法。

【請求項６】　暗号化された所定の情報を復号化する復号化方法において、
暗号化された所定の情報を受信し、
一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化することを特徴とする復号化方法。

【請求項７】　階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであり、
一方向関数を用いて上記マスターキーから暗号化キーに対応する復号化キーを生成することを特徴とする請求項６に記載の復号化方法。

【請求項８】　暗号化された特定情報を受信し、
暗号化されていない上記特定情報、暗号化された上記特定情報及び上記復号化キーを決定するための情報から上記復号化キーを決定し、
その決定された復号化キーを用いて上記暗号化された所定の情報を復号化することを特徴とする請求項６に記載の復号化方法。

【請求項９】　上記復号化キーを決定するための上記情報は、マスターキー、もしくは最新の暗号化キーの情報であることを特徴とする請求項８に記載の復号化方法。

【請求項１０】　上記復号化キーは、
上記復号化キーを決定するための上記情報を用いて、上記暗号化された特定情報を復号化するステップと、
その復号化された特定情報と暗号化されていない上記特定情報とを比較し、比較結果に基づいて上記復号化キーを決定するステップとにより決定されることを特徴する請求項８に記載の復号化方法。

2

【請求項１１】　復号化された上記特定情報と暗号化されていない上記特定情報とが一致しない場合、上記復号化キーを決定するための情報から、上記一方向関数を用いて階層化されている新たな上記復号化キーを求め、その新たな復号化キーを用いて、暗号化されている上記特定情報を復号化する動作を、復号化された上記特定情報と暗号化されていない上記特定情報とが一致するまで繰り返し、復号化された上記特定情報と暗号化されていない上記特定情報とが一致したとき、そのときの上記復号化キーを最終的な上記復号化キーとすることを特徴とする請求項１０に記載の復号化方法。

【請求項１２】　上記暗号化された所定の情報は、記録媒体に記録されており、その暗号化された所定の情報は、上記記録媒体から読み出されることにより供給され、
上記暗号化キーは、上記記録媒体または上記記録媒体を収納するケース上に上記暗号化キーに対応する文字、数字、バーコードもしくはホログラムとして印刷されていることを特徴する請求項６に記載の復号化方法。

【請求項１３】　上記暗号化キーは、暗号化された所定の情報を復号化するための所定のソフトウェアの中に、上記暗号化キーに対応するコードとして挿入されていることを特徴とする請求項６に記載の復号化方法。

【請求項１４】　上記暗号化キーは、電話回線、またはネットワークを介して供給されることを特徴する請求項６に記載の復号化方法。

【請求項１５】　所定の情報を所定の暗号化キーを用いて暗号化する暗号化装置において、
一方向関数を用いて階層化することにより上記暗号化キーを発生する発生手段と、
上記階層化された暗号化キーを用いて上記所定の情報を暗号化する暗号化手段とを有することを特徴とする暗号化装置。

【請求項１６】　階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであることを特徴とする請求項１５に記載の暗号化装置。

【請求項１７】　上記階層化された暗号化キーを用いて特定情報を暗号化する第２の暗号化手段をさらに有することを特徴とする請求項１５に記載の暗号化装置。

【請求項１８】　暗号化された所定の情報を復号化する復号化装置において、
暗号化された所定の情報を受信する受信手段と、
一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化する復号化手段とを有することを特徴とする復号化装置。

【請求項１９】　上記暗号化キーに対応する復号化キーを決定するための情報を記憶する第１の記憶手段と、
一方向関数を用いてマスターキーから上記暗号化キーに

対応する復号化キーを生成する生成手段と、
上記生成された暗号化キーに対応する復号化キーを記憶する第２の記憶手段とをさらに有し、
その暗号化キーに対応する復号化キーを決定するための情報は、階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーであるマスターキーであることを特徴とする請求項１８に記載の復号化装置。
【請求項２０】　上記受信手段は、暗号化された特定情報を受信し、
上記生成手段は、暗号化されていない上記特定情報、暗号化されている特定情報及び上記暗号化キーに対応する復号化キーを決定するための情報から、受信した上記所定の情報を暗号化した暗号化キーに対応する復号化キーを決定し、
上記復号化手段は、その決定された復号化キーを用いて上記暗号化された所定の情報を復号化することを特徴とする請求項１９に記載の復号化装置。
【請求項２１】　上記暗号化キーに対応する復号化キーを決定するための上記情報は、マスターキー、もしくは最新の暗号化キーの情報であることを特徴とする請求項２０に記載の復号化装置。
【請求項２２】　上記生成手段は、上記暗号化キーに対応する復号化キーを決定するための上記情報を用いて上記暗号化された特定情報を復号化し、その復号化された特定情報と上記特定情報とを比較し、比較結果に基づいて暗号化キーに対応する復号化キーを決定することを特徴する請求項２１に記載の復号化装置。
【請求項２３】　上記生成手段は、復号化された上記特定情報と暗号化されていない上記特定情報とが一致しない場合、上記復号化キーを決定するための情報から、上記一方向関数を用いて階層化されている新たな上記復号化キーを求め、その新たな復号化キーを用いて、暗号化されている上記特定情報を復号化する動作を、復号化された上記特定情報と暗号化されていない上記特定情報とが一致するまで繰り返し、復号化された上記特定情報と暗号化されていない上記特定情報とが一致したとき、そのときの上記復号化キーを上記第２の記憶手段に記憶させることを特徴とする請求項２２に記載の復号化装置。
【請求項２４】　上記第１の記憶手段、上記第２の記憶手段、上記生成手段、および上記復号化手段は、１つのＩＣチップ内に配置されていることを特徴とする請求項１９に記載の復号化装置。
【請求項２５】　上記暗号化キーに対応する復号化キーを決定するための情報は、予め第１の記憶手段に記憶されていることを特徴とする請求項２４に記載の復号化装置。
【請求項２６】　復号化装置によって復号可能な記録媒体において、
復号化装置によって復号可能な記録信号を有し、
上記記録信号は、一方向関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を含んでいることを特徴する記録媒体。
【請求項２７】　上記記録信号は、さらに、上記暗号化キーを用いて暗号化された特定情報を含んでいることを特徴とする請求項２６に記載の記録媒体。
【請求項２８】　上記暗号化キーは、上記記録媒体に上記暗号化キーに対応する文字、数字、バーコードもしくはホログラムとして印刷されていることを特徴する請求項２６に記載の記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録方法によって情報が記録された記録媒体に関し、例えば、ディジタル・ビデオ・ディスク（ＤＶＤ）などの記録媒体に記録されたソフトウェアもしくはデータ、またはネットワークを介して供給されるソフトウェアもしくはデータ等の不正使用を防止する場合に用いて好適な暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体に関する。
【０００２】
【従来の技術】通常、ソフトウェアやデータの不正使用を防止する場合、ソフトウェアやデータを所定の暗号化キーを用いて暗号化して、この暗号化されたソフトウェアまたはデータをディジタル・ビデオ・ディスク（以下、ＤＶＤと記述する）に記録したり、ネットワークを介して供給するようにしている。そして、ＤＶＤやネットワークを介して提供された暗号化されたソフトウェアまたはデータは、別途供給された上記暗号化キーを用いて復号化される。
【０００３】ここで、簡単に、情報の暗号化及び復号化について説明する。図１２は、情報の暗号化及び復号化に関しての原理を示している。送り側において、平文Ｍ（送信する情報）が暗号化鍵Ｋ１を用いて暗号化ブロック１０１で暗号化され、暗号文Ｃ（実際に送信されるデータ）が生成される。その暗号文Ｃが受け側に送信され、受け側において、復号化鍵K2を用いて復号化ブロック１０２で復号化され、平文Ｍが生成される。このようにして、平文が送り側から受け側に送られる。
【０００４】また、復号化鍵を有しない者（解読者）が暗号文Ｃを盗聴して、その暗号文Ｃを解読ブロック１０３で解読することがある。なお、ここで、復号化鍵を有する者が復号化鍵を用いて暗号文Ｃから平文Ｍを生成することを、“復号”と呼び、復号化鍵を有しない者が暗号文Ｃを盗聴して暗号文Ｃから平文を獲得することを、“解読”と呼ぶ。
【０００５】ところで、上述したような暗号化キーを用いて暗号化を行う場合、暗号化キー一度が解読されてしまうと、以後、この暗号化キーは、不正使用の防止に対しては無効になってしまう。そこで、暗号化キーが解読

されたときには、暗号化キーを別のものに更新し、新たな暗号化キーを用いてソフトウェアまたはデータの暗号化を行うことにより、その不正使用を防止するようにすることが考えられる。

【０００６】

【発明が解決しようとする課題】しかしながら、現実には、暗号化キーを更新しても、以前の暗号化キーで暗号化されたソフトウェアまたはデータが存在している場合があるので、その復号化のために以前の暗号化キーも保持しておかなければならない。このため、暗号化キーが更新される度に保持すべき暗号化キーが増加し、暗号化キーの管理がハードウェア的にも、ソフトウェア的にも容易ではなくなる課題があった。

【０００７】また、ハードウェア的に暗号化キーが予め組み込まれている場合、それを新たな暗号化キーに更新すること自体が極めて困難な場合がある。

【０００８】本発明は、このような状況に鑑みてなされたものであり、本発明の目的は、暗号化キーを階層化し、暗号化キーの管理を容易にする暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体を提供することにある。

【０００９】

【課題を解決するための手段】請求項１に記載の暗号化方法は、暗号化キーを一方向関数を用いて階層化し、階層化された暗号化キーを用いて所定の情報を暗号化することを特徴とする。

【００１０】請求項４に記載の記録方法は、一方向関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を受信し、暗号化された所定の情報を記録媒体に記録することを特徴とする。

【００１１】請求項６に記載の復号化方法は、暗号化された所定の情報を受信し、一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化することを特徴とする。

【００１２】請求項１５に記載の暗号化装置は、一方向関数を用いて階層化することにより暗号化キーを発生する発生手段と、階層化された暗号化キーを用いて所定の情報を暗号化する暗号化手段とを有することを特徴とする。

【００１３】請求項１８に記載の復号化装置は、暗号化された所定の情報を受信する受信手段と、一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化する復号化手段とを有することを特徴とする。

【００１４】請求項２６に記載の記録媒体は、復号化装置によって復号可能な記録信号を有し、記録信号は、一方向関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を含んでいることを特徴する。

【００１５】上記いずれの場合においても、暗号化キーとしては一方向関数で階層化されたものが用いられる。

【００１６】

【発明の実施の形態】図１は、本発明の暗号化方法を適用した暗号化キーの階層化の方法の例を示す図である。同図において、最初の階層の暗号化キー（マスタキー（Ｍａｓｔｅｒｋｅｙ）（Ｋ０））に対して、いわゆる一方向関数F（one-way Function）を用いて、次の階層（Ｖｅｒ．ｎ）の暗号化キーＫ１が形成される。ここで、F はいわゆる一方向関数の１つで、暗号化キーＫ０からＫ１を演算することは容易にできるが、その逆の演算、即ち、暗号化キーＫ１からＫ０を演算することは極めて困難であるような不可逆性の演算を行う関数である。

【００１７】一方向関数には、Data Encryption Standard (DES, National Bureau of Standards FIPS Publication 46, 1977) 、Fast Encryption Algorithm(FEAL, S.Miyaguchi. The FEAL cipher family. Lecture Notes in Computer Science, 537(1001), pp627-638. (Advances in Cryptology - CRYPTO '90)) のような暗号化アルゴリズム、あるいはMessage Digest algorithm (MD4, R. L. Rivest. The MD4 message digest algorithm. Lecture Notes in Computer Science, 537(1001), 303-311. (Advances in Cryptology - CRYPTO '90)) やSecure Hash Standard (SHS, Secure Hash Standard. National Bureau of Standards FIPS Publication 180, 1993) のようなメッセージダイジェストアルゴリズムを使用することができる。なお、ＤＥＳ、ＦＥＡＬに関しては、「辻井、笠原、「暗号と情報セキュリティ」、１９９３年７月」に詳細に記載されている。続いて、一方向関数について、例を挙げて簡単に説明する。

【００１８】ＤＥＳの場合、一方向関数とＤＥＳとの間には、次式（１）に示すような関係がある。即ち、

【００１９】

$$F(k) = DES(IV, k) \quad \cdots (1)$$

（ここで、ＩＶは、Ｉｎｉｔｉａｌ　Ｖｅｃｔｏｒであり任意、ｋは鍵）

である。

【００２０】また、一方向関数に使うアルゴリズムとしては、例えば、以下のようなものがある。

【００２１】・ｂｌｏｃｋ　ｃｉｐｈｅｒ（ｐｒｏｄｕｃｔ　ｃｉｐｈｅｒ）系のアルゴリズム。

・数論的アルゴリズム。

【００２２】ｂｌｏｃｋ　ｃｉｐｈｅｒ（ｐｒｏｄｕｃｔ　ｃｉｐｈｅｒ）系のアルゴリズムは、次式（２）に示すように、平文（Ｐｌａｉｎ　ｔｅｘｔ）を、鍵（ｋｅｙ）を用いて、暗号化し、暗号文（Ｃｉｐｈｅｒ　ｔｅｘｔ）を得る。

【００２３】

C＝Ｅｎｃ（Ｐ，ｋ）
（ただし、Ｃはｃｉｐｈｅｒ　ｔｅｘｔ、
Ｐはｐｌａｉｎ　ｔｅｘｔ、
ｋはｋｅｙ（鍵））

【００２４】即ち、ｋｅｙに対して、ブロック毎にあるｈａｓｈ　ｆｕｎｃｔｉｏｎにより、逆戻りできないような変換を施し、固定長のビット列を得る。

【００２５】次に、ｐｌａｉｎ　ｔｅｘｔをデータの置き換えなどを行うｐｅｒｍｕｔａｔｉｏｎ　ｂｏｘやｓｕｂｓｔｉｔｕｔｉｏｎ　ｂｏｘに数ラウンド通す。各

Ｆ（ｋ）＜＝＝＞a^k　ｍｏｄ　ｐ
（ただし、ａは所定の定数、ｋは鍵、ｐは素数）

・・・（２）

ラウンドで、ｋｅｙから得られたビット列とある種の演算、例えば排他的論理和演算（Ｅｘｏｒ）を施す。

【００２６】また、数論的アルゴリズムは、次式（３）に示すように、離散対数問題に使用される。

【００２７】

・・・（３）

【００２８】なお、上記式（３）において、記号「＜＝＝＞」は、「定義」を意味している。

【００２９】即ち、関数Ｆ（ｋ）を、「ａをｋ乗したものをｐで割った余り」と定義する。この場合、鍵（ｋ）からＦ（ｋ）は容易に求めることができるが、Ｆ（ｋ）からｋを求めるのは非常に困難である。

【００３０】このように、一方向関数（Ｆ）を用いてマスタキーＫ０から暗号化キーＫ１が求められた後、続いて、同様に一方向関数（Ｆ）を用いて、次式（４）に示すように、順次暗号化キーＫ２，Ｋ３，・・・Ｋｎ－１，Ｋｎが演算され、階層化（Ｖｅｒ．ｎ乃至Ｖｅｒ．１）された暗号化キーが形成される。

【００３１】

Ｋｉ＝Ｆ（Ｋｉ-1）（ただし、ｉ＝１，２，３，・・・，ｎ）　・・・（４）

【００３２】なお、数値ｎは、十分と考えられる階層の数（世代数）である。従って、上述したように、一方向関数（Ｆ）を用いて新たに暗号化キーを演算することは容易にできるが、その逆の演算、即ち、一方向関数を用いて演算された暗号化キーから元のキーを演算することは極めて困難である。

【００３３】ここで、本発明におけるソフトウェアまたはデータなどの情報を暗号化してユーザに提供する方法について説明する。ソフトウェアまたはデータ等の情報を暗号化してユーザに提供する場合、図１に示すように、最初に暗号化キーＫｎ（Ｖｅｒ．１）を用いて情報を暗号化し、暗号化キーＫｎを暗号化された情報に添付するか、もしくは別途供給するなどしてユーザに配布するようにする。ユーザは、暗号化された情報を、暗号化キーＫｎを用いて復号化することができる。

【００３４】そして、もし、この暗号化キーＫｎが解読された場合、ソフトウェアまたはデータ等の情報を１つ上の階層（Ｖｅｒ．２）の暗号化キーＫｎ－１を用いて暗号化し、暗号化キーＫｎ－１をユーザに配布するようにする。以下同様に、暗号化キーが解読される度に、解読された暗号化キーの１つ上の階層の暗号化キーを用いて情報を暗号化し、その暗号化キーをユーザに配布するようにする。

【００３５】例えば、最初に配布される最下位の階層（Ｖｅｒ．１）の暗号化キーＫｎは、次の階層（Ｖｅｒ．２）の暗号化キーＫｎ－１から関数Ｆを用いて演算されたものである。つまり、関数Ｆを用いることにより、暗号化キーＫｎ－１から暗号化キーＫｎを容易に演算することができ、暗号化キーＫｎ－１から演算された暗号化キーＫｎを用いて、暗号化キーＫｎによって暗号化された情報を復号化することができる。以下、同様に、どの世代においても、関数Ｆを用いることにより、次の暗号化キーを演算することができる。

【００３６】従って、ユーザは、解読されていない最新の暗号化キーを保持しておくだけで、最新の暗号化キーによって暗号化された情報だけでなく、以前の暗号化キーによって暗号化された情報も復号化することができる。また、すべての暗号化キーは、一方向性関数Ｆを用いて、マスターキーから順次生成されるキーである。従って、ユーザは、解読されていない最新の暗号化キーの代わりにマスターキーを保持しておくだけで、すべての暗号化キーによって暗号化された情報を復号化することができる。これにより、暗号化キーの管理を容易にすることができる。

【００３７】図２は、ディスクを作成する側において、図１に示した暗号化キーを用いて、例えば、ディスク（例えば、ＤＶＤ）等の記録媒体に、動画、音声、データ、ソフトウェアなどの情報（平文データ：Ｐｌａｉｎ　ｔｅｘｔ）を暗号化して記録するときの手順を説明するためのフローチャートである。最初に、ステップＳ１において、図１に示した階層化された暗号化キーのうち、適当な世代（階層）の暗号化キーを選択し、その選択された暗号化キーをワークキー（ｗｏｒｋ　ｋｅｙ）として選択する。次に、ステップＳ２に進み、予め決められた所定の数字や文字の列をマジック番号（ｍａｇｉｃ　ｎｕｍｂｅｒ）とし、そのマジック番号をステップ

Ｓ１で選択したワークキーを用いて暗号化する。そして、暗号化によって得られた暗号化されたマジック番号（ｅｎｃｒｙｐｔｅｄ　ｍａｇｉｃ　ｎｕｍｂｅｒ）が、図３に示すように、例えば、ＤＶＤ１の所定の場所に記録される。

【００３８】次に、ステップＳ３において、隠したい情報、つまり、平文データをワークキーを用いて暗号化し、暗号化された情報（ｃｉｐｈｅｒ　ｔｅｘｔ）をＤＶＤ１の所定の場所に記録する。

【００３９】次に、上述した暗号化方法に対応する暗号化装置を、図４を用いて説明する。平文データとマジック番号が、それぞれの入力端子を介して対応する暗号化回路５１または５２に供給される。ワークキー生成回路５３は、図１に示した階層化された暗号化キーのうち、適当な世代（階層）の暗号化キーを選択し、その選択された暗号化キーをワークキーとして、暗号化回路５１，５２に供給する。暗号化回路５２は、供給されたマジック番号をワークキー生成回路５３から供給されたワークキーを用いて暗号化する。そして、暗号化されたマジック番号が、記録装置５４に供給される。

【００４０】また、暗号化回路５１は、供給された平文データをワークキーを用いて暗号化し、暗号化された情報を記録装置５４に供給する。そして、記録装置５４は、暗号された情報及び暗号化されたマジック情報を、図３に示すように、例えば、ＤＶＤ１の所定の場所に記録する。なお、この記録装置５４がマスターディスクを生成するフォーマッタである場合には、その原盤からスタンパが形成され、その後、そのスタンパを使って、大量のディスクが生産される。

【００４１】図５は、上述したようにして作成されたＤＶＤ１を再生するディスクプレーヤー（ＤＶＤプレーヤー）において、ＤＶＤ１に記録された暗号化された情報の復号化を行うＩＣチップの構成例を示すブロック図である。ＩＣチップ１１には、マジック番号（ｍａｇｉｃ　ｎｕｍｂｅｒ）、暗号化されたマジック番号（ｅｎｃｒｙｐｔｅｄ　ｍａｇｉｃ　ｎｕｍｂｅｒ）および暗号化された情報（ｃｉｐｈｅｒ　ｔｅｘｔ）が入力されるようになされている。暗号化されたマジック番号としては、ＤＶＤ１から再生されたものが供給され、マジック番号としては、ＤＶＤプレーヤ自身が図示せぬメモリなどに保持していたものが、そのメモリから読み出されて供給される。このマジック番号は、予め決められた所定の数字や文字の列であり、暗号化側で使用されたマジック番号と同一のものである。

【００４２】メモリ１２は、図１に示した暗号化キーＫ０、即ち、マスターキーを保持するようになされている。レジスタ１３は、後述するようにして、マスターキーに対して上記関数Ｆを用いて求められた所定の世代の暗号化キー、即ちワークキー（ｗｏｒｋ　ｋｅｙ）を保持するようになされている。復号化回路１４は、後述するように、まず、入力されたマジック番号、暗号化されたマジック番号およびメモリ１２から読み出されたマスターキーに基づいて、ワークキーを作成し、その作成されたワークキーをレジスタ１３に供給するようになされている。そして、復号化回路１４は、入力された暗号化された情報（Ｃｉｐｈｅｒ　Ｔｅｘｔ）をワークキーを用いて復号化し、平文データ（Ｐｌａｉｎ　ｔｅｘｔ）として出力するようになされている。

【００４３】次に、図６に示したフローチャートを参照して、ＩＣチップ１１内におけるＤＶＤ１に記録された暗号化された情報を復号化する手順について説明する。最初に、ステップＳ１１において、ＤＶＤ１の所定の場所に記録された暗号化されたマジック番号が読み出される。次に、ステップＳ１２に進み、ステップＳ１１において読み出された暗号化されたマジック番号と、ＤＶＤプレーヤ自身が有する図示しないメモリから読み出されたマジック番号から、図７のフローチャートを参照して後述するようにしてワークキーを求める。

【００４４】図７は、図６のステップＳ１２における処理の詳細を説明するためのフローチャートである。最初に、ステップＳ２１において、ＩＣチップ１１のメモリ１２よりマスタキーが読み出され、これが選択キー（ｋ）とされる。そして、この選択キー（ｋ）が、復号化回路１４に供給される。ここで、選択キー（ｋ）は、現在選択されている暗号化キーを表すものとする。

【００４５】次に、ステップＳ２２に進み、復号化回路１４は、供給された、暗号化されているマジック番号（ＭＮｅ）を選択キー（ｋ）を用いて復号化する。そして、暗号化されているマジック番号を選択キー（ｋ）で復号化した結果とマジック番号とが一致するか否かを判定する。復号化した結果と暗号化されていないマジック番号とが一致しないと判定された場合、この選択キーは、暗号化側において、暗号化されたマジック番号を暗号化した暗号化キーではないと判定される。よって、ステップＳ２３に進み、次式（５）に示すように、選択キー（ｋ）から一方向関数（Ｆ）を用いて、次の世代の暗号化キーを演算し、それを新たに選択キー（ｋ）とする。

【００４６】ｋ＝Ｆ（ｋ）　・・・（５）

【００４７】そして、再び、ステップＳ２２に戻り、上述した場合と同様の処理を繰り返し実行する。

【００４８】一方、ステップＳ２２において、暗号化されているマジック番号を選択キー（ｋ）で復号化した結果と、暗号化されていないマジック番号が一致すると判定された場合、選択キー（ｋ）は、暗号化側において、暗号化されたマジック番号を暗号化した暗号化キーであると判定される、よって、ステップＳ２４に進み、復号化回路１４は、この選択キー（ｋ）をワークキーとし、それをレジスタ１３に供給し、レジスタ１３に記憶させる。そして、この図７のフローチャートの処理が終了さ

れ、図６のフローチャートの処理に戻る。

【００４９】その後、図６のフローチャートのステップＳ１３に進み、復号化回路１４は、ステップＳ１２（図７のステップＳ２１乃至２４）において求められたワークキーをレジスタ１３から読み出し、入力された暗号化されている情報（Ｃｉｐｈｅｒ　Ｔｅｘｔ）を、ワークキーを用いて復号化し、平文データ（Ｐｌａｉｎ　Ｔｅｘｔ）として出力する。

【００５０】このように、ＩＣチップ１１は、マスターキーから、暗号化された情報に対応するワークーキーを求め、入力された暗号化された情報をこのワークキーを用いて復号化するので、マスターキーを保持しておくだけで、任意の階層の暗号化キーによって暗号化された情報を復号化することができる。

【００５１】上述したような処理を、コンピュータのソフトウェアによって行う場合、図６のステップＳ１２の処理は、図８に示したようになる。即ち、図８は、図５に示したような機能をソフトウェアで実現するコンピュータにおいて、暗号化された情報が復号化される手順を示すフローチャートである。この場合、コンピュータは、図５に対応するような復号基板を内蔵しており、その基板のメモリにソフトウェアが記憶されている。また、この場合、予めメモリに記憶されているマスターキーを使用するのではなく、配布される最新の暗号化キー（マスターキーの場合もある）を使用する。

【００５２】例えば、図９を参照して後述するように、ＤＶＤに印刷されて配布された所定の階層の暗号化キー（Ｋｉ）（ここで、ｉはｎ，ｎ－１，・・・，１のいずれか）をユーザがキーボードを介してコンピュータに入力する。その暗号化キーが、コンピュータ内の所定のメモリに記憶されるようになされている。あるいは、コンピュータは、電話回線やネットワークを介して配布された最新の暗号化キーを受信し、それを所定のメモリ（例えば、ＲＡＭ）に記憶するようになされている。

【００５３】最初に、ステップＳ３１において、入力された所定の階層の暗号化キー（Ｋｉ）がメモリから読み出され、選択キー（ｋ）とされる。ここで、選択キー（ｋ）は、上述した場合と同様に、現在選択されている暗号化キーを表すものとする。

【００５４】次に、ステップＳ３２に進み、暗号化されているマジック番号が選択キー（ｋ）を用いて復号化される。そして、暗号化されているマジック番号を選択キー（ｋ）で復号化した結果とマジック番号とが一致するか否かが判定される。復号化した結果と暗号化されていないマジック番号とが一致しないと判定された場合、選択キー（ｋ）は、暗号化側において、マジック番号を暗号化した暗号化キーではないと判定される。よって、ステップＳ３３に進み、上記式（５）に示したように、選択キー（ｋ）から一方向関数（Ｆ）を用いて、次の世代の暗号化キーを演算し、それを新たに選択キー（ｋ）とする。

【００５５】そして、再び、ステップＳ３２に戻り、上述した場合と同様の処理を繰り返し実行する。

【００５６】一方、ステップＳ３２において、暗号化されているマジック番号を選択キー（ｋ）で復号化した結果とマジック番号とが一致すると判定された場合、選択キー（ｋ）は、暗号化側において、マジック番号を暗号化した暗号化キーであると判定される。よって、ステップＳ３４に進み、この選択キー（ｋ）をワークキーとし、このワークキーが所定のメモリ(例えば、レジスタ)に記憶される。そして、この図８のフローチャートの処理が終了され、図６のフローチャートの処理に戻る。

【００５７】その後は、図６のフローチャートのステップＳ１３に進み、ステップＳ１２（図８のステップＳ３１乃至Ｓ３４）において求められたワークキーを用いて、暗号化された情報を復号化し、平文データ（Ｐｌａｉｎ・Ｔｅｘｔ）として出力する。

【００５８】このように、暗号化されている情報の復号化を、コンピュータのソフトウェアで行う場合においては、配布された任意の階層の暗号化キーに基づいて、少なくともその暗号化キー（Ｋｉ）、またはその暗号化キーの階層よりも低い階層の暗号化キー（Ｋｉ－１乃至Ｋ１）によって暗号化されている情報を復号化することができる。

【００５９】このように、本発明の実施の形態においては、最新の暗号化キー（マスタキーの場合も有り得るし、任意の階層の暗号化キーの場合も有り得る）に基づいて、それ以前の暗号化キーによって暗号化された情報をも復号化することができるので、最新の暗号化キーだけを記憶しておけばよく、従来のように、暗号化キーが解読され、暗号化キーが変更される度に、それ以前の暗号化キーに加えて新たな暗号化キーを記憶し、管理する必要がなくなり、暗号化キーの管理を容易にすることができる。

【００６０】また、図５の実施の形態においては、暗号化キー（マスタキー）を、チップ１１のメモリ１２に記憶させ、そのチップ内で所定の階層の暗号化キーを演算し、暗号化された情報を復号化するようにしたので、暗号化キーが外部に漏れることを抑制することができ、暗号化キーの解読を困難にすることができる。さらに、上記実施の形態においては、ワークキーの算出処理と、暗号化された情報の復号化処理とを同一の復号化回路１４で行うようにしたので、構成を簡略化することができる。

【００６１】次に、図９乃至図１１を参照して、暗号化キーを配布する方法について説明する。

【００６２】図９は、暗号化キーをＤＶＤのケースやＤＶＤ自体に印刷して配布する例を示している。

【００６３】例えば、所定の階層の暗号化キーＡに対応するアルファベット文字、数字、バーコード、あるいは

ホログラム等を、タイトルＡが記録されたＤＶＤ２１のケースやＤＶＤ２１自体の表面等に印刷する。同様にして、所定の階層の暗号化キーＢに対応するアルファベット文字、数字、バーコード、あるいはホログラム等を、タイトルＢが記録されたＤＶＤ２２のケースやＤＶＤ２２自体の表面等に印刷する。このようにして、暗号化キーＡをＤＶＤ２１とともに、また、暗号化キーＢをＤＶＤ２２とともに、ユーザに配布することができる。

【００６４】あるいは、ＩＣカード等の記録媒体に暗号化キーＡを表すデータを記録してＤＶＤ２１とともに、また、ＩＣカード等の記録媒体に暗号化キーＢを表すデータを記録してＤＶＤ２２とともに配布するようにすることも可能である。

【００６５】ユーザは、ＤＶＤ２１を再生する場合、ＤＶＤ２１に印刷された暗号化キーＡを、コンピュータ２３にキーボード等の入力装置２４を用いて入力する。コンピュータ２３は、図８のフローチャートを参照して、上述したように、例えば、図５に示したＩＣチップ１１が行う機能、即ち暗号化された情報を復号化する機能を所定のアプリケーションプログラムによって実行するようになされている。

【００６６】次に、ＤＶＤ２１を図示せぬＤＶＤ読み取り装置にセットすると、コンピュータ２３は、ＤＶＤ読み取り装置を介して、ＤＶＤ２１から暗号化された情報を読み出し、先に入力された暗号化キーＡに基づいて、ＤＶＤ２１から読み出した暗号化されている情報を復号化する。ＤＶＤ２２についてもＤＶＤ２１の場合と同様にして、そこに記録された暗号化されている情報を復号化することができる。

【００６７】従って、この例は、ＤＶＤのタイトル毎に異なる暗号化キーを配布する場合、例えば、ＤＶＤのタイトル毎に、異なるマスタキーから一方向関数によって演算された暗号化キーを割り当てるような場合に適している。

【００６８】例えば、タイトルＡに対応する暗号化キーＡが解読され、タイトルＡに対応する暗号化キーＡが、その上の階層の暗号化キーＡ2に更新され、タイトルＡの続編が暗号化キーＡ2によって暗号化されている場合でも、更新される前の暗号化キーＡは、図８を参照して上述したように、暗号化キーＡ2から所定の演算によって容易に求めることができる。従って、ユーザは、最新の暗号化キー（この場合、暗号化キーＡ2）だけを用いて、以前の暗号化キーで暗号化されたタイトルＡをも復号化することができる。

【００６９】図１０は、暗号化キーを復号化するためのソフトウェアに、暗号化キーを表すコードを挿入して配布する例を示している。

【００７０】即ち、暗号化情報を復号化する復号化基板３３に設けられている復号化のためのソフトウェアの中に、暗号化キーを表すコードが挿入される。そして、この復号化基板３３をコンピュータ２３に装着する。これにより、コンピュータ２３は、ＤＶＤ３１，３２に記録された暗号化された情報を復号化基板３３を介して復号化することができ、復号化した情報に対応する動画、静止画、および音声などを出力することができる。

【００７１】この例は、ＤＶＤのタイトルに依らず、同一の暗号化キーを配布する場合に適している。

【００７２】また、この例の場合、コンピュータ２３を電話回線あるいはネットワークに接続し、更新した暗号化キーを電話回線あるいはネットワークを通じてコンピュータ２３に配布するようにすることも可能である。コンピュータ２３は、電話回線またはネットワークを介して配布された最新の暗号化キーを、復号化基板３３の復号化のためのソフトウェアの中に記憶させる。

【００７３】そして、コンピュータ２３は、この暗号化キーを用いて、図６および図８を参照して上述したようにして、ＤＶＤ３１，３２に記録された情報を復号化することができる。

【００７４】また、電話回線またはネットワークを介して暗号化キーによって暗号化した情報を伝送し、コンピュータ２３に提供するようにすることができる。この場合、コンピュータ２３は、先に電話回線またはネットワークを介して配布された暗号化キーを用いてこの情報を復号化する。

【００７５】ところで、図１を参照して上述したように、階層化した最初の暗号化キー（Ｋ０）から、一方向関数（Ｆ）を用いて全ての階層の暗号化キーを形成することができ、この暗号化キーＫ０をマスターキーとすることができる。そこで、このマスタキーとなる暗号化キーＫ０を、集積回路等のハードウェアの中に埋め込んでおくことにより、この暗号化キーＫ０から全ての階層の暗号化キーを作成することができ、どの暗号化キー（Ｋ１乃至Ｋｎ）で暗号化された情報でも復号化することができるようにすることができる。通常のユーザにとって、集積回路等のハードウェアに埋め込まれたデータを解読することは困難であるので、このようにして暗号化キーの不正使用を抑制することができる。

【００７６】図１１は、このように集積回路に暗号化キーを埋め込んで配布する例を示している。同図において、所定の守秘義務を有する製造者によって、マスタキーを記憶する集積回路４１が製造される。この集積回路４１には、例えば、図５に示したＩＣチップ１１を適用することができる。そして、この例の場合、この集積回路４１が製造者Ａに供給され、製造者ＡによってＤＶＤプレーヤ４３に組み込まれた後、ユーザに提供される。

【００７７】一方、ＤＶＤ４２には、集積回路４１が記憶する所定の階層の暗号化キーを用いて暗号化されたマジック番号、およびこの暗号化キーを用いて暗号化された所定の暗号化情報が記録される。

【００７８】ユーザが、ＤＶＤ４２をＤＶＤプレーヤ４

３にセットすると、集積回路４１からマスタキーが読み出され、図６および図７のフローチャートを参照して上述したようにして、ワークキーが求められ、ＤＶＤ４２に記録された暗号化された情報が復号化され、対応する動画、静止画、および音声が出力される。

【００７９】このように、集積回路４１にマスタキーを記憶させた場合、ＤＶＤプレーヤ４３は、ＤＶＤ４２に記録された情報がどの階層の暗号化キーによって暗号化されていたとしても、ＤＶＤ４２に記録された暗号化された情報を復号化して出力させることができる。

【００８０】また、集積回路４１にマスタキーではなく、マスタキーから一方向関数を用いて演算される暗号化キーのうちの所定の階層の暗号化キーを記憶させることもできる。その場合、その暗号化キーまたはその暗号化キーより低い階層の暗号化キーによって暗号化された情報がＤＶＤ４２に記録されているとき、ＤＶＤプレーヤ４３は、ＤＶＤ４２に記録されたその情報を復号化することができる。

【００８１】このように、所定の集積回路に所定の暗号化キーを記憶させ、それをＤＶＤプレーヤ４３に組み込む方法は、ＤＶＤのタイトルに依らず同一の暗号化キーを配布する場合に適している。

【００８２】以上のように、暗号化キーを一方向関数を用いて階層化し、階層化した暗号化キーのうち、任意の階層の暗号化キーを用いて情報を暗号化するとともに、この暗号化キーをユーザに配布することにより、ユーザは最新の暗号化キーを保持するだけで、以前の暗号化キーによって暗号化された情報も復号化することができる。これにより、暗号化キーを容易に管理することができる。

【００８３】例えば、図１１に示した実施の形態は、特に、ネットワーク等を介して暗号化キーのやりとりを容易に行うことができないような場合に、より有効に適用することができる。即ち、ＤＶＤ４２にソフトウェアや動画等の情報が所定の階層の暗号化キーによって暗号化されて記録されている場合において、集積回路４１はマスタキーを記憶しているので、このマスタキーから一方向関数（Ｆ）を用いて任意の階層の暗号化キーを作成することができ、ＤＶＤ４２に記録されている所定の階層の暗号化キーによって暗号化された情報を復号化することができる。

【００８４】これにより、ユーザは、暗号化キーが解読されるなどして更新され、ＤＶＤ４２に新たな階層の暗号化キーによって暗号化された情報が記録されたとしても、従来通り特に意識することなくそれを復号化して再生することができる。

【００８５】また、暗号化キーを記憶する集積回路４１を有していないＤＶＤプレーヤーにおいては、この暗号化キーによって暗号化された情報が記録されたＤＶＤ４２を正しく再生することができないので、情報の利用を適切に制限することができる。同様に、暗号化キーを記憶する復号基板を有していないコンピュータにおいては、この暗号化キーによって暗号化された情報が記録された記録媒体を正しく再生することができないので、情報の利用を適切に制限することができる。

【００８６】さらに、ＤＶＤなどの記録媒体またはそのケースに暗号化キーを表すアルファベット文字、数字、バーコード、あるいはホログラム等を印刷したり、ＩＣカードに暗号化キーに対応するデータを記憶させたり、不正使用が困難な集積回路内に暗号化キー（例えば、マスタキー）に対応するデータを記憶させたり、復号化のためのソフトウェアの中に暗号化キーに対応するデータを挿入したり、あるいは電話回線やネットワークを介して伝送するなどして、極めて容易に暗号化キーを配布することができる。

【００８７】なお、上記実施の形態においては、記録媒体としてＤＶＤを用いるようにしたが、勿論これに限定されるものではなく、ＣＤ－ＲＯＭ、ＭＤ（ミニディスク）（商標）、光ディスク、光磁気ディスク、またはフロッピディスク等のその他の記録媒体を用いるようにすることも可能である。

【００８８】また、本発明は、インターネット等のネットワークを介して、情報を提供する場合にも適用することが可能である。

【００８９】さらに、上記実施の形態においては、マジック番号をＤＶＤプレーヤ自身が所定のメモリ等に保持するようにしたが、例えば、ＤＶＤの所定の場所に記録し、それを読み出して復号化回路１４に入力させるようにすることも可能である。その場合、図４に示すように、マジック番号が記録装置５４に供給されて、ディスク１に記録される。また、コンピュータにおいて、暗号化されている情報をソフトウェアによって復号化するようになされているが、ソフトウェアを使用せずに、ＩＣチップをコンピュータに内蔵して、ＩＣチップに復号動作を行わせるようにしてもよい。この場合、暗号化キーを記憶する集積回路４１を有していないコンピュータは、暗号化された情報を正しく復号化することができないので、情報の利用を適切に制限することができる。

【００９０】なお、本発明の主旨を逸脱しない範囲において、さまざまな変形や応用例が考えうる。従って、本発明の要旨は、実施の形態に限定されるものではない。

【００９１】

【発明の効果】以上のごとく、請求項１に記載の暗号化方法、請求項４に記載の記録方法、請求項１５に記載の暗号化装置、および請求項２６に記載の記録媒体によれば、暗号化キーを一方向関数を用いて階層化するようにしたので、復号化側において、最新の暗号化キーを保持するだけで、古い暗号化キーで暗号化された情報をも復号化することができ、暗号化キーが更新された場合における暗号化キーの世代管理を容易にすることが可能とな

る。

【００９２】また、請求項６に記載の復号化方法、および請求項１８に記載の復号化装置によれば、一方向関数を用いて階層化された暗号化キーを用いて復号化を行うようにしたので、最新の暗号化キーを保持するだけで、古い暗号化キーで暗号化された情報をも復号化することができる。

【図面の簡単な説明】

【図１】本発明の暗号化方法に適用される暗号化キーの階層構造の例を示す図である。

【図２】暗号化した情報を記録したＤＶＤを作成する手順を示すフローチャートである。

【図３】暗号化されたマジックキーと暗号化された情報が記録されたＤＶＤを示す図である。

【図４】本発明における暗号化装置の構成例を示すブロック図である。

【図５】図３のＤＶＤに記録された情報を復号化するチップ１１の構成例を示すブロック図である。

【図６】図５のチップ１１の動作を説明するためのフローチャートである。

【図７】図６のステップＳ１２の詳細を説明するためのフローチャートである。

【図８】図６のステップＳ１２の詳細を説明するための他のフローチャートである。

【図９】暗号化キーをＤＶＤに印刷して配布する方法を説明するための図である。

【図１０】暗号化キーを復号化のためのソフトウェアに挿入して配布する方法を説明するための図である。

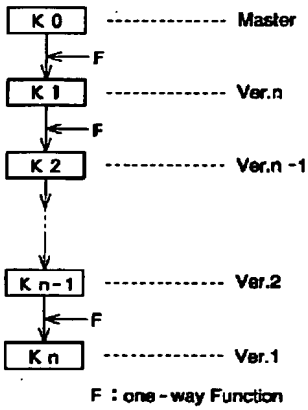
【図１１】集積回路に暗号化キーを埋め込んで配布する方法を説明するための図である。

【図１２】暗号化及び復号化の原理を示す図である。

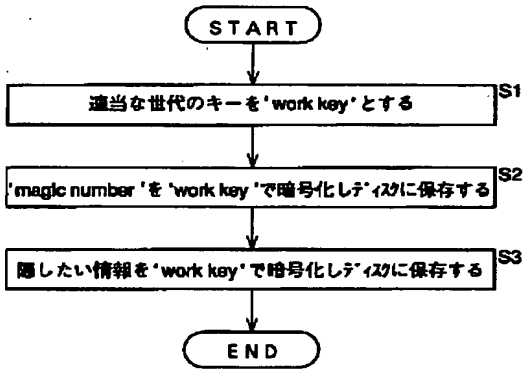
【符号の説明】

１　ディスク，　１１　チップ，　１２　メモリ，　１３　レジスタ，　１４復号化回路，　２１，２２　ＤＶＤ，　２３　コンピュータ，　３１，３２ＤＶＤ，　３３　復号化基板，　４１　集積回路，　４２　ＤＶＤ，　４３　ＤＶＤプレーヤ

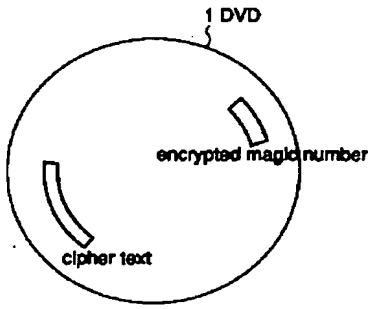
【図１】



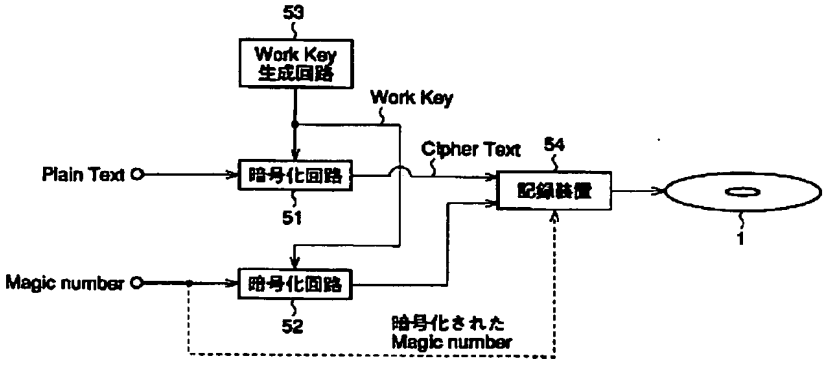
【図２】



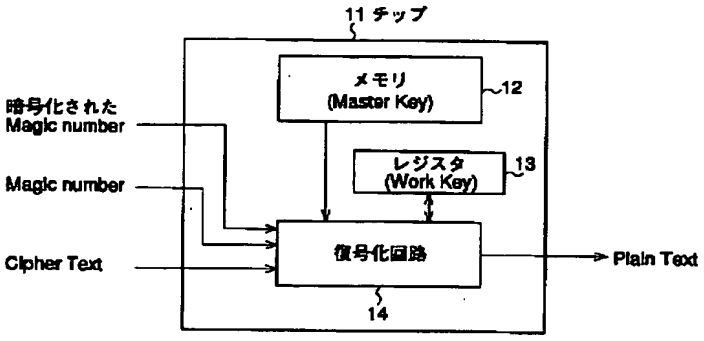
【図３】



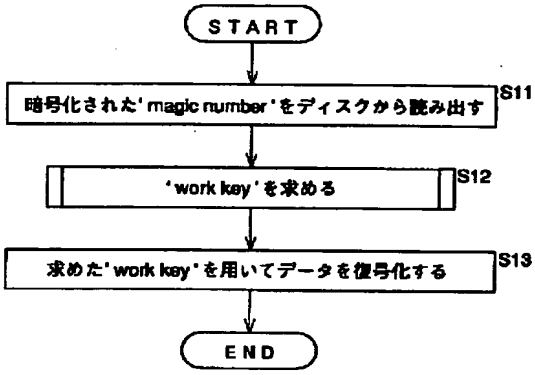
【図４】



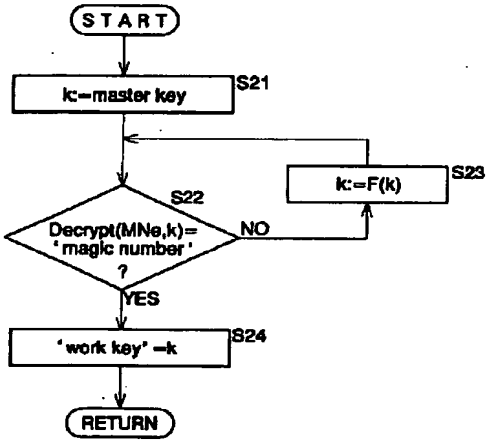
【図５】


11 チップ
メモリ
(Master Key)
12
暗号化された
Magic number
レジスタ
(Work Key)
13
Magic number
復号化回路
Cipher Text
Plain Text
14

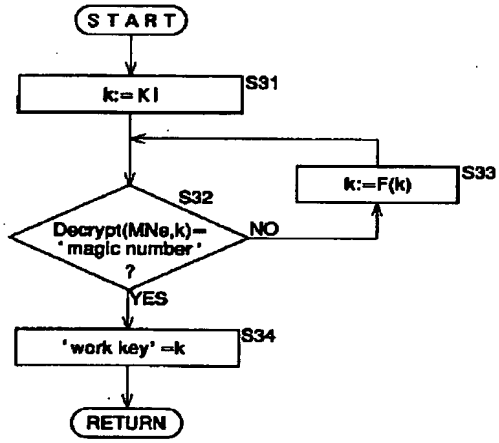
【図６】


START
暗号化された' magic number 'をディスクから読み出す
S11
' work key ' を求める
S12
求めた' work key ' を用いてデータを復号化する
S13
END

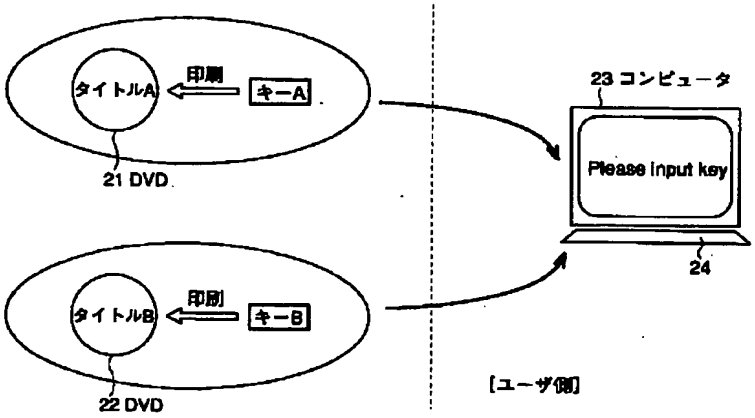
【図７】


START
k:=master key
S21
k:=F(k)
S23
S22
Decrypt(MNe,k)=
' magic number '
?
NO
YES
' work key' =k
S24
RETURN

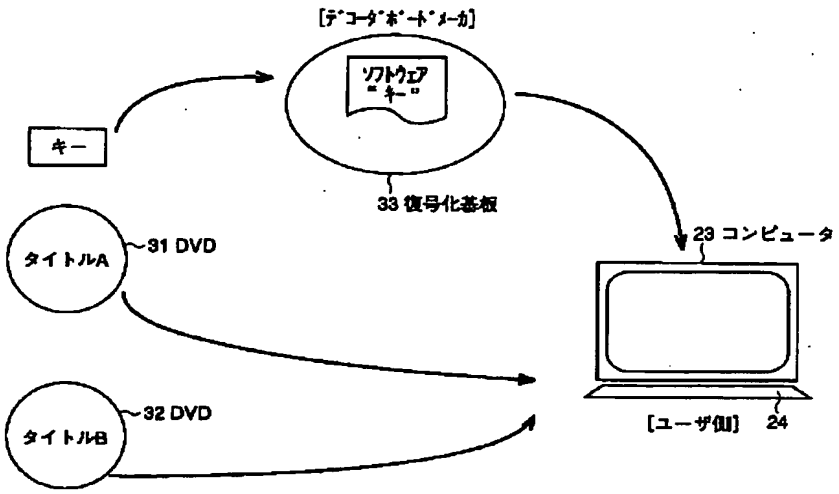
【図８】


START
k:= KI
S31
k:=F(k)
S33
S32
Decrypt(MNe,k)=
' magic number '
?
NO
YES
' work key' =k
S34
RETURN

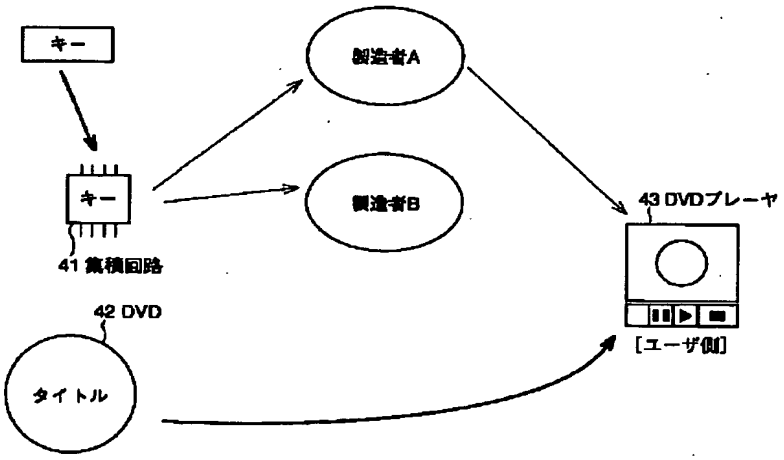
【図９】


タイトルA
印刷
キーA
21 DVD
タイトルB
印刷
キーB
22 DVD
23 コンピュータ
Please Input key
24
[ユーザ側]

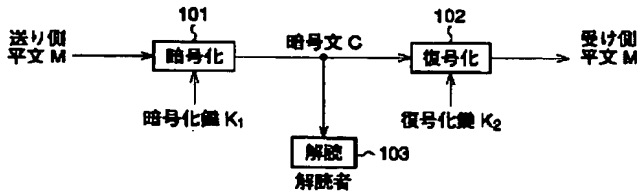
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ 9/00	６０１Ａ	
	9/06				６１１Ａ	